IN THE CLAIMS:

Please amend the claims as follows:

1. (Cancelled)

2. (Previously Presented) An apparatus for use in one of: secret communications by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, the apparatus comprising a machine readable memory that provides instructions for solving a system of linear equations $Ax=b$ in n unknowns on a finite field $GF(p)$, where p is a prime, n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, which when executed by a machine, cause said machine to perform operations comprising:

reading a stored coefficient matrix A and a stored constant vector b, and triangular transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements;

calculating inverses of diagonal elements of the generated coefficient matrix C on the finite field $GF(p)$; and

solving the system of linear equations $Cx=d$ using the generated coefficient matrix C, the generated constant vector d, and the calculated inverses of the diagonal elements of the generated coefficient matrix C, to thereby solve the system of linear equations $Ax=b$ of the read coefficient matrix A and the read constant vector b; and

performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the solution of the system of linear equations $Ax=b$; wherein

the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without a division on the finite field $GF(p)$ being performed;

generating the coefficient matrix C and the constant vector d of the system of linear equations $Cx=d$ from the coefficient matrix A and the constant vector b of the system of linear equations $Ax=b$ includes one or more successive transformation processes;

the system of linear equations $Ax=b$ is subjected to the first transformation process and the system of linear equations $Cx=d$ is generated as a result of the last transformation process;

in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation;

in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

each transformation process has a same number of transformation subprocesses as the one or more object equations, each for transforming a separate one of the one or more object equations into an equation equivalent to the object equation; and

in each transformation subprocess,

(a) each of the coefficients and a constant in the pivotal equation is multiplied by a nonzero coefficient chosen from the object equation, and values

generated as a result of the multiplications are set into a second coefficient group,

(b) each of coefficients and a constant in the object equation is multiplied by a nonzero coefficient chosen from the pivotal equation, and values generated as a result of the multiplications are set into a first coefficient group, and

(c) the values in the second coefficient group are subtracted respectively from the values in the first coefficient group, and differences generated as a result of the subtractions are respectively set as coefficients and a constant in the equation equivalent to the object equation.

3. (Cancelled)

4. (Previously Presented) The apparatus of Claim 2, wherein

when the diagonal elements of the coefficient matrix C are denoted by m_i $(i=1,2,...,n)$ and the inverses of the diagonal elements m_i $(i=1,2,...,n)$ in the finite field $GF(p)$ are denoted by I_i $(i=1,2,\ldots,n)$, calculating inverses of diagonal elements of the coefficient matrix C includes

(a) computing values t and t_i where

$$t_i = \prod_{k=1}^{n} m_k \text{ (except } m_i) \bmod p \ (i=1,2,\ldots,n)$$

and

$$t = \prod_{k=1}^{n} m_k \bmod p$$

(b) computing u where

$u=1/t \bmod p$

and

(c) computing values I_i where

$I_i = u \times t_i \bmod p\ (i=1,2,\ldots,n)$

to find the inverses $I_i\ (i=1,2,\ldots,n)$.

5. (Currently Amended) The apparatus of Claim 4,

wherein computing the values t and t_i includes calculating

$s_1 = m_1 \times m_2 \bmod p$

$s_2 = s_1 \times m_3 \bmod p$

[[⋮]]

$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$

in the stated order, then calculating

$t_n = s_{n-3} \times m_{n-1} \bmod p$

$t_{n-1} = s_{n-3} \times m_n \bmod p$

$s_n = m_{n-1} \times m_n \bmod p$

$t_{n-2} = s_{n-4} \times s_n \bmod p$

$s_{n-1} = m_{n-2} \times s_n \bmod p$

$t_{n-3} = s_{n-5} \times s_{n-1} \bmod p$

$s_{n-2} = m_{n-3} \times s_{n-1} \bmod p$

$t_{n-4} = s_{n-6} \times s_{n-2} \bmod p$

[[⋮]]

$s_5 = m_4 \times s_6 \bmod p$

$t_3 = s_1 \times s_5 \bmod p$

$s_4 = m_3 \times s_5 \bmod p$

$t_2 = m_1 \times s_4 \bmod p$

$t_1 = m_2 \times s_4 \bmod p$

in the stated order, and lastly calculating

$t = t_j \times m_j$

for a value j chosen from a set of positive integers $\{1, 2, \ldots, n\}$.

6. (Previously Presented) An apparatus for use in one of: secret communications by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, the apparatus comprising a machine readable memory that provides instructions for solving a system of linear equations $Ax=b$ in n unknowns on a finite field $GF(p)$, where p is a prime, n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, which when executed by a machine, cause said machine to perform operations comprising:

reading a stored coefficient matrix A and a stored constant vector b, and triangular transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements;

calculating inverses of diagonal elements of the generated coefficient matrix C on the finite field $GF(p)$; and

solving the system of linear equations $Cx=d$ using the generated coefficient matrix C, the generated constant vector d, and the calculated inverses of the diagonal elements of the generated coefficient matrix C, to thereby solve the system of linear equations $Ax=b$ of the read coefficient matrix A and the read constant vector b; and

performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the solution of the system of linear equations $Ax=b$; wherein

the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without a division on the finite field $GF(p)$ being performed;

generating the coefficient matrix C and the constant vector d of the system of linear equations $Cx=d$ from the coefficient matrix A and the constant vector b of the system of linear equations $Ax=b$ includes one or more successive transformation processes;

the system of linear equations $Ax=b$ is subjected to the first transformation process and the system of linear equations $Cx=d$ is generated as a result of the last transformation process;

in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation;

in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

each transformation process has a coefficient group calculation process and a same number of transformation subprocesses as the one or more object equations, the transformation subprocesses being performed following the coefficient group calculation process and being each for transforming a separate one of the one or more object equations;

in the coefficient group calculation process,

(a) a nonzero coefficient is chosen from each of the pivotal equation and the one or more object equations, a product is calculated for each of the pivotal equation and the one or more object equations by multiplying together all chosen nonzero coefficients except a nonzero coefficient chosen from the equation, and products calculated respectively for the pivotal equation and the one or more object equations are set into a first coefficient group, and

(b) each of coefficients and a constant in the pivotal equation except a nonzero coefficient chosen from the pivotal equation in the coefficient group calculation process is multiplied by a product in the first coefficient group calculated for the pivotal equation, and values generated as a result of the multiplications are set into a second coefficient group; and

in each transformation subprocess for transforming a separate one of the one or more object equations,

(a) a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to *0* as a new coefficient,

(b) each of coefficients in the object equation except the nonzero coefficient chosen from the object equation is multiplied by a product in the first coefficient group calculated for the object equations, values in the second coefficient group calculated from the coefficients in the pivotal equation are subtracted respectively from values generated as a result of the multiplications on the coefficients in the object equation to generate differences, and the coefficients in the object equation are changed respectively to the differences as new coefficients, and

(c) a constant in the object equation is multiplied by the product calculated for the object equations, a value in the second coefficient group calculated from the constant in the pivotal equation is subtracted from a value generated as a result of the multiplication on the constant in the object equation to generate a difference, and the constant in the object equation is changed to the difference as a new constant.

7. (Previously Presented) The apparatus of Claim 2,

wherein when the diagonal elements of the coefficient matrix C are denoted by m_i $(i=1,2,...,n)$ and the inverses of the diagonal elements m_i $(i=1,2,...,n)$ in the finite field $GF(p)$ are denoted by I_i $(i=1,2,...,n)$, calculating inverses of diagonal elements of the coefficient matrix C includes

(a) a multiplying unit for computing values t and t_i where

$$t_i = \prod_{k=1}^{n} m_k \ (except\ m_i)\ mod\ p\ (i=1,2,\ldots,n)$$

and

$$t = \prod_{k=1}^{n} m_k \ \text{mod p}$$

(b) computing a value u where

$u=1/t$ mod p

and

(c) computing values I_i where

$I_i = u \times t_i$ mod p (i=1,2,...,n)

to find the inverses I_i $(i=1,2,...,n)$.

8. (Currently Amended) The apparatus of Claim 7,

wherein computing values t and t_i includes calculating

$s_1=m_1 \times m_2\ mod\ p$

$s_2=s_1 \times m_3\ mod\ p$

[[⋮]]

$s_{n-3}=s_{n-4} \times m_{n-2}\ mod\ p$

in the stated order, then calculating

$t_n = s_{n-3} \times m_{n-1} \; mod \; p$

$t_{n-1} = s_{n-3} \times m_n \; mod \; p$

$s_n = m_{n-1} \times m_n \; mod \; p$

$t_{n-2} = s_{n-4} \times s_n \; mod \; p$

$s_{n-1} = m_{n-2} \times s_n \; mod \; p$

$t_{n-3} = s_{n-5} \times s_{n-1} \; mod \; p$

$s_{n-2} = m_{n-3} \times s_{n-1} \; mod \; p$

$t_{n-4} = s_{n-6} \times s_{n-2} \; mod \; p$

[[⋮]]

$s_5 = m_4 \times s_6 \; mod \; p$

$t_3 = s_1 \times s_5 \; mod \; p$

$s_4 = m_3 \times s_5 \; mod \; p$

$t_2 = m_1 \times s_4 \; mod \; p$

$t_1 = m_2 \times s_4 \; mod \; p$

in the stated order, and lastly calculating

$t = t_j \times m_j$

for a value j chosen from a set of positive integers $\{1,2,...,n\}$.

9. (Previously Presented) An apparatus for computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where p is a prime, $q=p^n$, and n is a positive integer, the apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; wherein

the equation solving means includes a machine readable memory that provides instructions for solving the system of linear equations $Ax=b$ where A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, which when executed by a machine, cause said machine to perform operations comprising

reading a stored coefficient matrix A and a stored constant vector b,

triangular transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements, wherein the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without a division on the finite field $GF(p)$ being performed,

calculating inverses of diagonal elements of the generated coefficient matrix C on the finite field $GF(p)$, and

solving the system of linear equations $Cx=d$ using the generated coefficient matrix C, the generated constant vector d, and the calculated inverses of the diagonal elements of the generated coefficient matrix C, to thereby

solve the system of linear equations $Ax=b$ of the read coefficient matrix A and the read constant vector b.

10. (Currently Amended) The apparatus of claim 2, the apparatus computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where $q=p^n$, the apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse I.

11. (Cancelled)

12. (Previously Presented) The apparatus of claim 4, the apparatus computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where $q=p^n$, the apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b-using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, ..., n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the-machine readable memory;

and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+...+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, ..., n-1)$ found by the equation solving means; and

means for performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse I.

13. (Previously Presented) The apparatus of claim 5,-the apparatus computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where $q=p^n$, the apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, ..., n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory;

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+...+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, ..., n-1)$ found by the equation solving means; and

means for performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse I.

14. (Previously Presented) The apparatus of claim 6, the apparatus computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where $q=p^n$, the apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse I.

15. (Previously Presented) The apparatus of claim 7, the apparatus computing an inverse I of an element y in $GF(q)$ which is an extension field of a finite field $GF(p)$, where $q=p^n$, the apparatus comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse *I*.

16. (Previously Presented) The apparatus of claim 8, the apparatus computing an inverse *I* of an element *y* in *GF(q)* which is an extension field of a finite field *GF(p)*, where $q=p^n$, the apparatus comprising:

equation generating means for generating the coefficient matrix *A* and the constant vector *b* using the element *y* and all coefficients of a generator polynomial of *GF(q)* whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse *I*, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse *I*.

17. (Previously Presented) A record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve *E* over *GF(q)* as a basis for security and recorded on a record medium, an inverse *I* of an element *y* in *GF(q)* to decrypt the encrypted digital content recorded on the record medium, where *GF(q)* is an extension field of a finite field *GF(p)*, *p* is a prime, $q=p^n$, *n* is a positive integer, and *G* is a base point of the elliptic curve *E*, the record medium reproducing apparatus comprising:

equation generating means for generating a coefficient matrix A and a constant vector b for a system of linear equations $Ax=b$ in n unknowns, using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium; wherein

the equation solving means includes a machine readable memory that provides instructions for solving the system of linear equations $Ax=b$ where A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, which when executed by a machine, cause said machine to perform operations comprising

reading a stored coefficient matrix A and a stored constant vector b,

triangular transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements, wherein the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without a division on the finite field $GF(p)$ being performed,

calculating inverses of diagonal elements of the generated coefficient matrix C on the finite field $GF(p)$, and

solving the system of linear equations $Cx=d$ using the generated coefficient matrix C, the generated constant vector d, and the calculated inverses of the diagonal elements of the generated coefficient matrix C, to thereby solve the system of linear equations $Ax=b$ of the read coefficient matrix A and the read constant vector b.

18. (Previously Presented) The apparatus of claim 2 wherein the apparatus is a record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of [[a]] <u>the</u> finite field $GF(p)$, $q=p^n$, and G is a base point of the elliptic curve E, the record medium reproducing apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the-machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium.

19. (Cancelled)

20. (Previously Presented) The apparatus of claim 4 wherein the apparatus is a record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis

for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of the finite field $GF(p)$, $q=p^n$, and G is a base point of the elliptic curve E, the record medium reproducing apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium.

21. (Previously Presented) The apparatus of claim 5, wherein the apparatus is a record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of the finite field $GF(p)$, $q=p^n$, and G is a base point of the elliptic curve E, the record medium reproducing apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium.

22. (Currently Amended) The apparatus of claim 6, wherein the apparatus is a record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of the finite field $GF(p)$, $q=p^n$, and G is a base point of the elliptic curve E, the record medium reproducing apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, \ldots, n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium.

23. (Previously Presented) The apparatus of claim 7, wherein the apparatus is a record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an

extension field of the finite field $GF(p)$, $q=p^n$, and G is a base point of the elliptic curve E, the record medium reproducing apparatus further comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, ..., n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+...+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, ..., n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium.

24. (Previously Presented) The apparatus of claim 8, wherein the apparatus is a record medium reproducing apparatus for computing, when copyrighted digital content has been encrypted using a discrete logarithm problem on an elliptic curve E over $GF(q)$ as a basis for security and recorded on a record medium, an inverse I of an element y in $GF(q)$ to decrypt the encrypted digital content recorded on the record medium, where $GF(q)$ is an extension field of the finite field $GF(p)$, $q=p^n$, and G is a base point of the elliptic curve E, the record medium reproducing apparatus comprising:

equation generating means for generating the coefficient matrix A and the constant vector b using the element y and all coefficients of a generator polynomial of $GF(q)$ whose root is α;

equation solving means for finding solutions x_k $(k=0, 1, 2, ..., n-1)$ of the system of linear equations $Ax=b$, the equation solving means including the machine readable memory; and

inverse computing means for computing the inverse I, $I=x_0+x_1\alpha+\ldots+x_{n-1}\alpha^{n-1}$, using the root α and the solutions x_k $(k=0, 1, 2, \ldots, n-1)$ found by the equation solving means; and

means for using I to decrypt the encrypted digital content recorded on the record medium.

25. (Cancelled)

26. (Previously Presented) A machine based method for use in one of: secret communications by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, the method solving a system of linear equations $Ax=b$ in n unknowns on a finite field $GF(p)$ where p is a prime, n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, the method comprising:

utilizing a machine readable memory to provide instructions to a machine for execution by the machine, wherein

the instructions, when executed by the machine, cause the machine to perform operations comprising:

reading a stored coefficient matrix A and a stored constant vector b, and triangular transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements;

calculating inverses of diagonal elements of the generated coefficient matrix C on the finite field $GF(p)$; and

solving the system of linear equations $Cx=d$ using the generated coefficient matrix C, the generated constant vector d, and the calculated inverses of the diagonal elements of the generated coefficient matrix C, to thereby solve the system of linear

equations $Ax=bi$ of the read coefficient matrix A and the read constant vector b, and

performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the solution of the system of linear equations $Ax=b$; wherein

the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without a division on the finite field $GF(p)$ being performed;

generating the coefficient matrix C and the constant vector d of the system of linear equations $Cx=d$ from the coefficient matrix A and the constant vector b of the system of linear equations $Ax=b$ includes one or more successive transformation processes;

the system of linear equations $Ax=b$ is subjected to the first transformation process and the system of linear equations $Cx=d$ is generated as a result of the last transformation process,

in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

each transformation process has a same number of transformation subprocesses as the one or more object equations, each for transforming a separate one of the one or more object equations into an equation equivalent to the object equation; and

in each transformation subprocess,

(a) each of the coefficients and a constant in the pivotal equation is multiplied by a nonzero coefficient chosen from the object equation, and values

generated as a result of the multiplications are set into a second coefficient group,

(b) each of coefficients and a constant in the object equation is multiplied by a nonzero coefficient chosen from the pivotal equation, and values generated as a result of the multiplications are set into a first coefficient group, and

(c) the values in the second coefficient group are subtracted respectively from the values in the first coefficient group, and differences generated as a result of the subtractions are respectively set as coefficients and a constant in the equation equivalent to the object equation.

27. (Cancelled)

28. (Previously Presented) The method of Claim 26, wherein

when the diagonal elements of the coefficient matrix *C* are denoted by m_i $(i=1,2,\ldots,n)$ and the inverses of the diagonal elements m_i $(i=1,2,\ldots,n)$ in the finite field *GF(p)* are denoted by I_i $(i=1,2,\ldots,n)$, calculating the inverses of the diagonal elements of the coefficient matrix *C* includes

(a) computing values t and t_i where

$$t_i = \prod_{k=1}^{n} m_k \ (except\ m_i)\ mod\ p\ (i=1,2,\ldots,n)$$

and

$$t = \prod_{k=1}^{n} m_k \ mod\ p$$

(b) computing value u where

$u=1/t \ mod\ p$

and

(c) computing values I_i where

$I_i = u \times t_i \bmod p \ (i=1,2,\ldots,n)$

to find the inverses $I_i \ (i=1,2,\ldots,n)$.

29. (Currently Amended) The method of Claim 28,

wherein the computing the values t and t_i includes calculating

$s_1 = m_1 \times m_2 \bmod p$

$s_2 = s_1 \times m_3 \bmod p$

[[⋮]]

$s_{n-3} = s_{n-4} \times m_{n-2} \bmod p$

in the stated order, then calculating

$t_n = s_{n-3} \times m_{n-1} \bmod p$

$t_{n-1} = s_{n-3} \times m_n \bmod p$

$s_n = m_{n-1} \times m_n \bmod p$

$t_{n-2} = s_{n-4} \times s_n \bmod p$

$s_{n-1} = m_{n-2} \times s_n \bmod p$

$t_{n-3} = s_{n-5} \times s_{n-1} \bmod p$

$s_{n-2} = m_{n-3} \times s_{n-1} \bmod p$

$t_{n-4} = s_{n-6} \times s_{n-2} \bmod p$

[[⋮]]

$s_5 = m_4 \times s_6 \bmod p$

$t_3 = s_1 \times s_5 \bmod p$

$s_4 = m_3 \times s_5 \bmod p$

$t_2 = m_1 \times s_4 \bmod p$

$t_1 = m_2 \times s_4 \bmod p$

in the stated order, and lastly calculating

$t = t_j \times m_j$

for a value j chosen from a set of positive integers $\{1, 2, \ldots, n\}$.

30. (Previously Presented) A machine based method for use in one of: secret communications by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, the method solving a system of linear equations $Ax=b$ in n unknowns on a finite field $GF(p)$ where p is a prime, n is a positive integer, A is a coefficient matrix consisting of elements of n rows and n columns, x is a vector of unknowns consisting of n elements, and b is a constant vector consisting of n elements, the method comprising:

utilizing a machine readable memory to provide instructions to a machine for execution by the machine, wherein

the instructions, when executed by the machine, cause the machine to perform operations comprising:

reading a stored coefficient matrix A and a stored constant vector b, and triangular transforming the read coefficient matrix A and constant vector b to generate a coefficient matrix C and a constant vector d for a system of linear equations $Cx=d$ in n unknowns that is equivalent to the system of linear equations $Ax=b$, the coefficient matrix C consisting of elements of n rows and n columns and the constant vector d consisting of n elements;

calculating inverses of diagonal elements of the generated coefficient matrix C on the finite field $GF(p)$; and

solving the system of linear equations $Cx=d$ using the generated coefficient matrix C, the generated constant vector d, and the calculated inverses of the diagonal elements of the generated coefficient matrix C, to thereby solve the system of linear

equations $Ax=bi$ of the read coefficient matrix A and the read constant vector b, and

performing one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the solution of the system of linear equations $Ax=b$; wherein

the coefficient matrix A is triangular transformed into the coefficient matrix C of upper triangular form without a division on the finite field $GF(p)$ being performed;

generating the coefficient matrix C and the constant vector d of the system of linear equations $Cx=d$ from the coefficient matrix A and the constant vector b of the system of linear equations $Ax=b$ includes one or more successive transformation processes;

the system of linear equations $Ax=b$ is subjected to the first transformation process and the system of linear equations $Cx=d$ is generated as a result of the last transformation process;

in each transformation process, a coefficient matrix and a constant vector of a system of linear equations in n unknowns are transformed into a coefficient matrix and a constant vector of a system of linear equations in n unknowns that is equivalent to the system of linear equations before the transformation;

in each transformation process, one pivotal equation which is a linear equation in n unknowns serving as a pivot for the transformation and one or more object equations which are linear equations in n unknowns to be transformed are chosen from the system of linear equations in n unknowns that is subjected to the transformation;

each transformation process has a coefficient group calculation process and a same number of transformation subprocesses as the one or more object equations, the transformation subprocesses being performed following the coefficient group calculation process and being each for transforming a separate one of the one or more object equations;

in the coefficient group calculation process,

(a) a nonzero coefficient is chosen from each of the pivotal equation and the one or more object equations, a product is calculated for each of the pivotal equation and the one or more object equations by multiplying together all chosen nonzero coefficients except a nonzero coefficient chosen from the equation, and products calculated respectively for the pivotal equation and the one or more object equations are set into a first coefficient group, and

(b) each of coefficients and a constant in the pivotal equation except a nonzero coefficient chosen from the pivotal equation in the coefficient group calculation process is multiplied by a product in the first coefficient group calculated for the pivotal equations, and values generated as a result of the multiplications are set into a second coefficient group; and

in each transformation subprocess for transforming a separate one of the one or more object equations,

(a) a nonzero coefficient chosen from the object equation in the coefficient group calculation process is changed to *0* as a new coefficient,

(b) each of coefficients in the object equation except the nonzero coefficient chosen from the object equation is multiplied by a product in the first coefficient group calculated for the object equations, values in the second coefficient group calculated from the coefficients in the pivotal equations are subtracted respectively from values generated as a result of the multiplications on the coefficients in the object equation to generate differences, and the coefficients in the object equation are changed respectively to the differences as new coefficients, and

(c) a constant in the object equation is multiplied by the product calculated for the object equations, a value in the second coefficient group calculated from the constant in the pivotal equation is subtracted from a value generated as a result of the multiplication on the constant in the object equation to

generate a difference, and the constant in the object equation is changed to the difference as a new constant.

31. (Previously Presented) The method of Claim 26, wherein

when the diagonal elements of the coefficient matrix C are denoted by m_i $(i=1,2,...,n)$ and the inverses of the diagonal elements m_i $(i=1,2,...,n)$ in the finite field $GF(p)$ are denoted by I_i $(i=1,2,...,n)$, calculating the inverses of the diagonal elements of the coefficient matrix C includes

(a) computing values t and t_i where

$$t_i = \prod_{k=1}^{n} m_k \text{ (except } m_i) \bmod p \ (i=1,2,...,n)$$

and

$$t = \prod_{k=1}^{n} m_k \bmod p$$

(b) computing a value u where

$u=1/t \bmod p$

and

(c) computing values I_i where

$I_i=u\times t_i \bmod p \ (i=1,2,...,n)$

to find the inverses I_i $(i=1,2,...,n)$.

32. (Currently Amended) The method of Claim 31,

wherein computing values t and t_i involves calculating

$s_1=m_1\times m_2 \bmod p$

$s_2=s_1\times m_3 \bmod p$

[[⋮]]

$$s_{n-3}=s_{n-4}\times m_{n-2} \mod p$$

in the stated order, then calculating

$$t_n=s_{n-3}\times m_{n-1} \mod p$$

$$t_{n-1}=s_{n-3}\times m_n \mod p$$

$$s_n=m_{n-1}\times m_n \mod p$$

$$t_{n-2}=s_{n-4}\times s_n \mod p$$

$$s_{n-1}=m_{n-2}\times s_n \mod p$$

$$t_{n-3}=s_{n-5}\times s_{n-1} \mod p$$

$$s_{n-2}=m_{n-3}\times s_{n-1} \mod p$$

$$t_{n-4}=s_{n-6}\times s_{n-2} \mod p$$

[[⋮]]

$$s_5=m_4\times s_6 \mod p$$

$$t_3=s_1\times s_5 \mod p$$

$$s_4=m_3\times s_5 \mod p$$

$$t_2=m_1\times s_4 \mod p$$

$$t_1=m_2\times s_4 \mod p$$

in the stated order, and lastly calculating

$$t=t_j\times m_j$$

for a value j chosen from a set of positive integers $\{1,2,\ldots,n\}$.